62/133,173, filed on Mar. 13, 2015, and U.S. application Ser. No. 15/066,945, both of which are hereby incorporated by reference in their entirety. In some embodiments, the ePM system **132** can be used to generate and verify barcodes or other computer or machine readable identifier attached to physical ballots that are sent out to allow users to vote by mail. In some embodiments, these barcodes or other computer or machine readable identifier can then be used to electronically submit votes in elections and to certify that voters submitted their results.

[0057] In some embodiments, the blockchain access layer **101** is in communication with a tokenizer vault **133**. Tokenizer vault **133** tokenizes an individual ballot cast by a voter. In order to cast a vote in the digital system the voter must be assigned a token corresponding to the election by the tokenizer vault **133**. In some embodiments, the token can also correspond to a particular EPM® associated with a voter. This enables the submission of a physical ballot by mail in an anonymous manner and the simultaneous creation of a digitized version using blockchain technology for added security.

[0058] In some embodiments, tokenizer vault **133** can issue multiple tokens that perform these functions. For example, the tokenizer vault **133** can issue separate ballot and obfuscation tokens. In some embodiments, a ballot token is a unique identifier that is generated for a specific user who signs up for voting in absentia in a specific election and is printed on the mailed ballot. This token authorizes the voter to one ballot submission for that election.

[0059] In some embodiments, the tokenizer vault **133** can also issue pseudo-anonymous obfuscation tokens to voters. In some embodiments, in order to cast a vote in the digital system, the voter must be assigned an obfuscation token corresponding to the election by the tokenizer vault **133**. In some embodiments, the obfuscation token is issued using an acceptable algorithm to represent an anonymized ID of the voter that is securely stored by a Key Management Service/Key Vault. All user transactions are subsequently anonymized and recorded on the blockchain using the token. The obfuscation token can be a type of a Zero Knowledge Proof identifier. In some embodiments, the obfuscation token can also correspond to a particular EPM® associated with a voter.

[0060] In some embodiments, the blockchain access layer **101** is in communication with a mailed ballot processor **134**. In some embodiments, the mailed ballot processor **134** can be used to analyze and identify ballots received by mail. In some embodiments, mail ballot processor **134** can read barcodes or other computer or machine-readable identifiers attached to physical ballots that are sent out to allow users to vote by mail and determine information about the received ballot. For example, the mailed ballot processor **134** can determine if a mailed ballot was received in time for the votes to count in the election based on the time that the machine-readable identifier was scanned by a mail processing system. In some embodiments, the mail ballot processor **134** can also be used to determine which entity should count a particular received ballot or to which entity, location, or facility the mailed ballot should be returned. For example, some elections may require that the ballots be counted by a local state or county authority. In some embodiments, the mail ballot processor **134** can determine the appropriate entity based on the machine-readable identifier. For example, the mail ballot processor **134** can determine the address of the voter based on the machine readable identifier and then determine that votes from that address should be sent to be counted at a particular county or state office. The mail ballot processor could then direct the mailed in ballot to be sent on to the appropriate office.

[0061] Item processing equipment, such as mail processing equipment can scan the physical documents, such as the ballots, ballet access token documents, and the like as they are moved through the distribution network. The distribution network can prove the tracking information to the system **100** to track the location of ballot and ballot related documents, to confirm delivery of the documents, and/or to provide predictive arrival dates and times. In some embodiments, the distribution network resources, such as carriers, can scan codes on the ballots as they are delivered in order to provide a positive delivery scan for the ballots or other election or voting documents to the system **100**.

[0062] In some embodiments, the blockchain access layer **101** can be in communication with oracles **141**. In some embodiments, oracles **141** are software services responsible for communicating and interfacing with systems outside of the blockchain powered voting system and then input information from those systems into the blockchain access layer. In some embodiments, oracles **141** can communicate with blockchain access layer **101** through a software API. In some embodiments, this API can be REST-API or RabbitMQ. In some embodiments, the oracles **141** can communicate with various state level election systems. For example, oracles **141** can interact with a voter registry **142**. Voter registry **142** can be a database that contains all of the voters that are registered to vote in that state. In some embodiments, oracles **141** can interact with a received ballots database **143**. In some embodiments, this database contains information on all of the voting ballots received by the state. In some embodiments, this information can then be transferred into and stored in voter-ballot database **154**, as discussed below. Oracles **141** can also interact with a jurisdiction election database **144**. Jurisdiction election database **144** contains all the information on what elections are happening in the jurisdiction. In some embodiments, this includes what positions are up for election and who the candidates are for each position.

[0063] In some embodiments, the blockchain access layer **101** is in communication with databases **150**. In some embodiments, databases **150** can store the various information that is received by the blockchain access layer **101**. In some embodiments, the databases **150** can contain all of the information that is not contained on the blockchain itself. In some embodiments, databases **150** are maintained and hosted by a single entity, such as the United States Postal Service. In some embodiments, databases **150** can contain an identity management services database **151**. In some embodiments, identity management services database **151** can contain all of the information on the voters that is received by blockchain access layer **101**, both from the voters directly through user interface **131**, and through identity services **130**.

[0064] In some embodiments, databases **150** can contain a ballot database **152**. The ballot database **152** can contain all the information on a generic, or template, ballot that is received by the blockchain access layer **101**. For example, the database can contain information on specific ballot templates that show the various categories and sub-categories of the open positions and the candidates (including their